BEÜ Fen Bilimleri Dergisi
10 (4), 1603-1614, 2021
DOI: 10.17798/bitlisfen.988001

BEU Journal of Science
10 (4), 1603-1614, 2021

Araştırma Makalesi / Research Article

Web Sitelerinde Gerçekleştirilen Oltalama Saldırılarının Yapay Zekâ Yaklaşımı ile Tespiti

Mesut TOĞAÇAR*

Fırat Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Elazığ
(ORCID: 0000-0002-8264-3899)

Öz
Oltalama, kişisel bilgilerin internet üzerinden çalınmasına yönelik gerçekleştirilen yazılım tabanlı saldırılardır. Oltalama saldırılarında genellikle kişilerin kimlik bilgileri, kullanıcı parolaları, kredi veya banka kartı bilgileri gibi özel bilgilerin ele geçirilmesi amaçlanır. Bunun için en uygun ortam olarak genelde özel yazılım kodları içeren web sitesi uygulamaları veya elektronik posta sistemleri tercih edilir. Bu tür net uygulamalarında gelen cezbedici görsel veya metin tabanlı iletiler bireyleri yemleyerek saldırıların gerçekleştirilmesini sağlar. Milyarlarca insanın etkileşim içerisinde olduğu internet ortamında bu tür saldırıların önlemini zamanında alabilmek için teknolojik gelişmelerle paralel hareket etmek gerekir. Son zamanlarda, yapay zekâ teknolojileri internet güvenliği alanında adını duyurmayı başarmıştır. Bu çalışmada, makine öğrenme yöntemleri ile 11 binin üzerinde web sitesi incelenmiş ve oltalama saldırısı yapan web siteleri tespit edildi. Veri seti, 30 web parametresinden oluşmaktadır ve açık erişimlidir. Makine öğrenmesi yöntemleri ile her bir web sitesi için 30 özellik incelendi; oltalama saldırısını gerçekleştiren web siteleri ile gerçekleştirmeyen web siteleri sınıflandırıldı. Sonuç olarak, en iyi test doğruluk başarısı Rastgele Orman yöntemi ile %96,53 oranında gerçekleştirildi.

Anahtar kelimeler: Kimlik avı dolandırıcılığı, Yapay zekâ, Makine öğrenmesi, Oltalama saldırıları.

Detection of Phishing Attacks on Websites Using Artificial Intelligence Approach

Abstract
Phishing is software-based attacks on the stealing of personal information over the internet. In phishing attacks, it is generally aimed to capture private information such as personal identification information, user passwords, credit or debit card information. Website applications or electronic mail systems containing special software codes are generally preferred as the most suitable medium for this. In this kind of net applications, attractive visual or text based messages feed individuals and enable attacks. It is necessary to act in parallel with the technological developments in order to prevent such attacks on time in the internet environment where billions of people interact. Recently, artificial intelligence technologies have managed to make a name in the field of internet security. In this study, over 11 thousand websites were analyzed with machine learning methods and websites that made phishing attacks were determined. The dataset consists of 30 web parameters and is open access. With machine learning methods, 30 features were examined for each website; web sites that carry out the phishing attack and those that did not. As a result, the best test accuracy achievement was realized by Random Forest method at 96.53%.

Keywords: Phishing scams, Artificial intelligence, Machine learning, Phishing attacks.

1. Giriş

Oltalama saldırıları, web uygulamaları üzerinde kullanıcıların kişisel bilgilerini, banka kartı veya kredi kartı bilgilerini, sosyal medya bilgilerini, şifrelerini almaya yönelik hazırlanmış eski ve etkili elektronik dolandırıcılık yöntemlerinden biridir [1]. Genellikle internet kullanıcıların elektronik postalarına gönderdikleri cezbedici içerik ve başlıklarla yemleme amaçlanır. Bunun dışında web uygulamalarında

* Sorumlu yazar: mtogacar@firat.edu.tr
Geliş Tarihi: 27.08.2021, Kabul Tarihi: 15.10.2021

kurumsal veya özel firmaların sayfa içeriklerini taklit ederek oltalamak istedikleri kullanıcı kitlelerini düşürülmeye çalışılır. Kısacası bu saldırılar oltalamaya çalışacakları kullanıcıları sosyal mühendislik yöntemlerini de kullanarak kullanıcı adları, numaraları veya şifrelerini ele geçirmeye çalışan kötü amaçlı yazılımlardır [2]. Verizon adlı firmanın 2019 yılı veri araştırmaları raporuna göre veri ihlallerinin yaklaşık %33,33 oranında oltama saldırılarından kaynaklandığını belirtmektedir. Amerika Federal Soruşturma Bürusu'nun İnternet Şikâyet Birimi'nin istatistik bilgilerine göre oltalama saldırıları ile işlenen suçların 2016-2019 yılı arasında vermiş olduğu maddi kayıp dünya genelinde 26 milyar $ üzerinde olduğunu belirtti. Ayrıca, 2020 yılında Google firması korona virüs (COVID-19) etiketini kullanarak aylık 240 milyona yakın spam iletisini engellediğini bildirdi [3]. IBM Güvenlik Raporunun 2020 yılı istatistik bilgisine göre veri ihlallerinin en çok yapıldığı sektör olarak sağlık alanı gelmektedir [4]. Bu tür durumların önüne geçebilmek için yapay zekâ tabanlı teknolojiler internet ortamında kullanılmaya başlamıştır.

Bu çalışmalardan bazıları incelenirse; Ping Yi vd. [5] çalışmasında derin inanç ağlarını kullanarak web sitelerinin kimlik avı gerçekleştirme durumlarını tespit etmişlerdir. Onlar çalışmasında web sitelerin İnternet Protokol (İP) adreslerini veri seti olarak kullanmışlardır. Kullandıkları modelde sınıflandırma yöntemi için Boltzmann makine öğrenme yöntemini kullanmışlardır. Sonuç olarak elde ettikleri sınıflandırma başarısı %89,6'dı. Bo Wei vd. [2] çalışmasında web sitelerin iyi ya da kötü amaçlı olduklarını tespit etmişlerdir. Bunun için derin öğrenme modeli tasarlamışlardır ve kullandıkları modelde sınıflandırıcı işlevini sigmoid fonksiyonu ile gerçekleştirmişlerdir. Onlar, çalışmanın analizinde %86,63 oranında bir doğruluk başarısı elde ettiler. Mustafa Kaytan vd. [6] çalışmasında Aşırı Öğrenme Makinelerini (AÖM) kullanarak oltama saldırılarının gerçekleştiği web sitelerin ayırt edilmesini gerçekleştirdiler. Onlar veri setini çapraz doğrulama yöntemi ile sınıflandırma sürecine katkıda bulundular ve elde ettikleri sınıflandırma başarısı %95,93'tü. Gunikhan Sonowal vd. [7] çalışmasında ikili özellik seçme yöntemini kullanarak elektronik postalar üzerinden gelen oltama saldırılarının tespitini gerçekleştirdiler. Onlar, özellik seçim algoritması ile elde ettikleri özellikleri Rastgele Orman (RO) yöntemi ile sınıflandırarak %97,41 oranında başarı elde etmişlerdir.

Bu makalenin amacı, kimlik avı dolandırıcılığında kullanılan oltalama saldırılarının tespitini makine öğrenme yöntemlerini kullanarak tespitini başarılı bir şekilde gerçekleştirmektir. Ayrıca, oltalama saldırılarının tespitinde makine öğrenme yöntemlerinden elde edilen analiz sonuçlarını kıyaslatmaktır. Çalışmanın diğer bölümleri şu şekildedir; deneysel analizlerde kullanılan veri seti ile ilgili bilgiler ikinci bölümde verilmiştir. Deneysel analizinde kullanılan makine öğrenme yöntemleri hakkında bilgiler üçüncü bölümde verilmiştir. Çalışmanın analiz sonuçları hakkında bilgiler dördüncü bölümde yer almıştır. Sırasıyla, Tartışma ve Sonuç bölümü son iki bölümü oluşturmuştur.

2. Veri Seti

Veri seti, 11055 web sitesi içeriğini barındıran; metin tabanlı ve "csv" uzantılı iki dosyadan oluşmaktadır. Her bir web sitesinin 30 özellik içeren parametresi vardır ve bu parametrelerin etiket grupları {-1, 1 } ile {-1, 0, 1 } değerler arasında oluşmaktadır. Parametre değeri olarak kullanılan 30 özellik ile ilgili bilgiler Tablo 1'de verilmiştir. Veriler, ikili sınıflandırma modeli için tasarlanmış ve oltalama saldırılarının gerçekleştiği web siteleri ile gerçekleştirilmeyen web sitelerinden oluşmaktadır. Veri seti, Kaggle web sitesinden erişime sunulmuştur [8].

Tablo 1. Veri setini oluşturan web sitelerinin parametreleri ve etiket değerleri

Özellik No	Web Sitesi Parametreleri	Etiket Değeri	Özellik No	Web Sitesi Parametreleri	Etiket Değeri
1	UsingIP	{-1, 0, 1 }	16	ServerFormHandler	{-1, 1 }
2	LongURL	{-1, 0, 1 }	17	InfoEmail	{-1, 1 }
3	ShortURL	{-1, 1 }	18	AbnormalURL	{-1, 1 }
4	Symbol@	{-1, 1 }	19	WebsiteForwarding	{-1, 0, 1 }
5	Redirecting//	{-1, 1 }	20	StatusBarCust	{-1, 1 }
6	PrefixSuffix-	{-1, 1 }	21	DisableRightClick	{-1, 1 }
7	SubDomains	{-1, 0, 1 }	22	UsingPopupWindow	{-1, 1 }
8	HTTPS	{-1, 0, 1 }	23	IframeRedirection	{-1, 1 }
9	DomainRegLen	{-1, 1 }	24	AgeofDomain	{-1, 1 }
10	Favicon	{-1, 1 }	25	DNSRecording	{-1, 0, 1 }
11	NonStdPort	{-1, 1 }	26	WebsiteTraffic	{-1, 1 }
12	HTTPSDomainURL	{-1, 1 }	27	PageRank	{-1, 1 }
13	RequestURL	{-1, 1 }	28	GoogleIndex	{-1, 0, 1 }
14	AnchorURL	{-1, 0, 1 }	29	LinksPointingToPage	{-1, 1 }
15	LinksInScriptTags	{-1, 0, 1 }	30	StatsReport	{-1, 1 }

Bu çalışmada veri seti iki aşamaya ayrılarak incelendi. İlk aşamada veri setinin %30'u test verisi %70'i eğitim verisi olarak ayrıldı. Test verisi olarak ayrılan web sitesi sayısı 3317'di. Test verilerinin 1479'u oltalama saldırılarının gerçekleştiği web siteleridir. İkinci aşamada ise, veri setine çapraz doğrulama uygulandı. Çapraz doğrulama oranı (k=5) seçilerek deney analizi gerçekleştirildi.

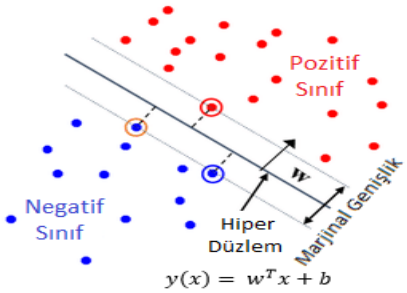
3. Makine Öğrenme Yöntemleri ve Önerilen Yaklaşım

3.1. Destek Vektör Makineleri Yöntemi

Destek Vektör Makineleri (DVM) yöntemi, regresyon ve sınıflandırma işlemleri için kullanılan makine öğrenme yöntemlerinden biridir. DVM sınıflandırma sürecinde verilerden çıkartılan özellikleri, ikiye bölecek şekilde bir sınır çizgisi kullanır. Şekil 1 incelendiğinde, hiper düzlem üzerinde marjinal genişlik boşluğu (w) optimizasyon yöntemi tarafından oluşturulur. Sınıflandırma sürecinde oluşabilecek problemleri minimize edebilmek için izlenecek işlem adımları Denklem 1 ve Denklem 2'de gösterildi. Denklemler incelendiğinde x ve y parametresi verilerden çıkartılmış özelliklerin koordinatlarını temsil eder. Ayrıca, sınır alanını b parametresi ve i ise döngü sayısını ifade eder. DVM yöntemi ile sınıflandırma aşamasında işlenen her bir özellik için sınıf sayısını temsil edecek şekilde olasılık değerleri aktarılır. Özelliğin temsil ettiği veri, olasılık değeri yüksek olan sınıfa atanır [9, 10].

$$u = w \cdot x - b \tag{1}$$

$$y_i (w \cdot x_i - b) \geq 1, \forall i \tag{2}$$



Şekil 1. DVM yönteminin sınıflandırma süreci

Bu çalışmada, Sklearn kütüphanesinde doğrusal DVM yöntemi kullanılarak analizler gerçekleştirildi. DVM yöntemi için tercih edilen diğer önemli parametreler; maksimum iterasyon sayısı 1000 seçildi, kesme ölçeklemesi değeri bir seçildi ve tolerans parametre değeri 10^{-4} seçildi.

3.2. En Yakın Komşu Yöntemi

EYK yöntemi, denetimli öğrenme modeli içerisinde yer alan ve girdi verilerini algoritma modelinde sınıflandırma problemini çözebilen makine öğrenme yaklaşımıdır. Sınıflandırma sürecinde veri özelliklerine benzerlikler gösteren özellikler aynı sınıfta etiketlenir. Bunu hesaplarken örnek bir veri özellikleri rastgele seçilir ve diğer verilerin özelliklerinin örnek veri özelliklerine göre uzaklıkları hesaplanır [11]. Sonuç olarak, "k" sayısı kadar yakın komşuluklarına bakılır. Burada k parametresi genelde $\{2,3,5,7, \dots\}$ gibi değerler seçilir. EYK yönteminin dezavantajı, her bir özellik verisi için uzaklık bilgilerinin tutulacağı bir bellek gereksinimine ihtiyacı olmasıdır. Özellikler arasında uzaklık ölçümleri için; “Euclidean”, “Manhattan”, “Minkowski” yöntemlerinden biri tercih edilmektedir [12].

Bu çalışmada, Sklearn kütüphanesinin desteklediği EYK yöntemi kullanıldı. Uzaklık ölçümü için Minkowski yöntemi kullanıldı ve k değeri beş seçildi.

3.3. Karar Ağacı Yöntemi

Karar Ağacı (KA) yöntemi, yapısı içerisinde kök, karar ve yaprak düğümlerinden oluşan sınıflandırma işlemlerinde tercih edilen bir makine öğrenme yaklaşımıdır. Sınıflandırma sürecinde, düğümler öz-yinelemeli yöntemler ile alt düğümlere ayrılır ve bu durum sınıflandırma sürecine etki etmeyene kadar devam eder. Sınıflandırma işleminde veri özelliklerinin ayırt edilebilmesini sağlamak için bilgi kazancı ölçümü denilen "Entropi" yöntemi kullanılır [13]. Entropi yöntemi ile verilerin belirsizlikleri ölçülür ve veri özellikleri elde edilen olasılık değerleri ile sınıflandırılır. Entropi (E) ölçümü için kullanılan formül Denklem 3'te verildi. Denklem 3’te N değişkeni veri sayısını ifade ederken; P ise i. verinin olasılık değerini ifade eder [14].

$$E = -\sum_{i=1}^{N} P_i \log_2 P_i \tag{3}$$

Bu çalışmada, KA yöntemi için tercih edilmiş diğer önemli parametreler; ölçüt değeri "gini" seçildi, maksimum derinlik değeri 30 seçildi. Diğer parametre değerleri ise Sklearn kütüphanesinde kabul edilmiş varsayılan değerlerdir.

3.4. Rastgele Orman Yöntemi

Rastgele Orman (RA) yöntemi, regresyon ve sınıflandırma işlemlerinde kullanılan makine öğrenme yaklaşımıdır. RA yöntemi, birden fazla karar ağacı kümesini oluşturur ve ardından bu kümeleri birleştirerek sınıflandırma sürecine daha doğru karar vermesini sağlar. Mümkün olduğunca farklı karar ağaçlarının bir araya getirilmesini amaçlar ve böylece düşük korelasyon içeren bir orman topluluğu oluşturulur [15]. Sınıflandırma sürecinde, rastgele düğümler seçilir ve rastgele seçilmiş değişkenler arasında da en iyi düğüm seçilir. Sınıfların homojenliğini ölçmek için "gini" parametresi kullanılır. Alt

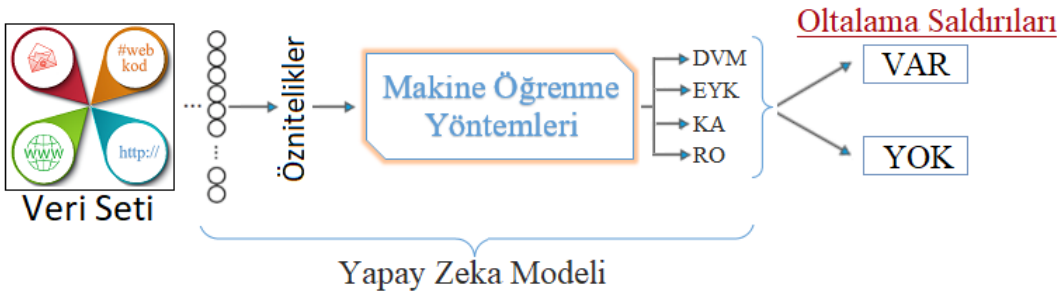
düğümün "gini" ölçüm değeri, üst düğümün "gini" ölçüm değerinden daha düşükse düğümlerin bulunduğu dal başarılı sayılır. Gini ölçümü Denklem 4'e göre hesaplanır. Tüm veriler N değişkeni ile temsil edilir ve seçilmiş veri ise n ile temsil edilir. Ayrıca, p_i değişkeni seçilmiş verinin kendisinden küçük ve kendisinden büyük eleman sayısına bölümünün karesini temsil eder [16].

$$Gini(N) = 1 - \sum_{i=1}^{n} {p_i}^2 \tag{4}$$

Bu çalışmada, RO yöntemi için tercih edilmiş diğer önemli parametreler; ölçüt değeri "gini" seçildi, maksimum derinlik değeri 30 seçildi. Diğer parametre değerleri ise Sklearn kütüphanesinde kabul edilmiş varsayılan değerlerdir.

3.5. Önerilen Yaklaşım

Önerilen yaklaşım, internet ortamı üzerinde kullanıcıların bilgilerini ele geçirmeye yönelik gerçekleştirilen oltalama saldırılarının tespitini gerçekleştirmektedir. Dolayısıyla, bu tür zararlı yazılımlar web uygulamaları, elektronik postalar gibi net ortamlarından uygulandığı için çalışmanın deneysel analizi binlerce web sayfaları ile gerçekleştirildi ve yapay zekâ teknolojisinin analiz sürecini başarılı bir şekilde gerçekleştirilmesi amaçlandı. Veri setinde, yer alan her bir web sayfasında 30 özellik içermektedir. Her bir web sitesinin özellik setini makine öğrenme yöntemlerine girdi olarak verildiği zaman, hangi web sitesinin güvenilir olup olmadığını başarılı bir şekilde tespit edilmesi gerçekleştirilmektedir. Önerilen yaklaşımın tasarımı Şekil 2'de gösterildi.



Şekil 2. Oltalama saldırıların tespitinde kullanılmak için tasarlanmış yapay zekâ destekli yaklaşımın genel tasarımı

4. Deneysel Sonuçlar

Deneysel analizler Python yazılım kodları kullanılarak gerçekleştirildi. Yazılım kodları, Github web sitesinde erişime sunulmuştur ve kaynak kodlardan esinlenerek önerilen yaklaşım tasarlandı [17]. Donanımsal gereksinimler için ve kodların derlenmesi için "Google Colab" sunucusu kullanıldı [18]. Makine öğrenme yöntemlerinin sınıflandırma başarılarının karşılaştırılmasında karmaşıklık matrisi kullanılmıştır. Karmaşıklık matrisinin ölçüm metrikleri ise şunlardır; özgünlük (Özg), kesinlik (Kes), geri Çağırma (Geri Çğr), f-skoru (F-skr) ve doğruluk (Dğr). Metrik sonuçlarının hesaplanmasında, Denklem 5 ile Denklem 9 arasındaki tüm denklemler kullanıldı. Denklemlerde kullanılan değişkenler; doğru pozitif (DP), doğru negatif (DN), yanlış pozitif (YP), yanlış negatif (YN) verilerin sayısı anlamına gelmektedir [19,20].

$$\text{Özg} = \frac{\text{DN}}{\text{DN+YP}} \tag{5}$$

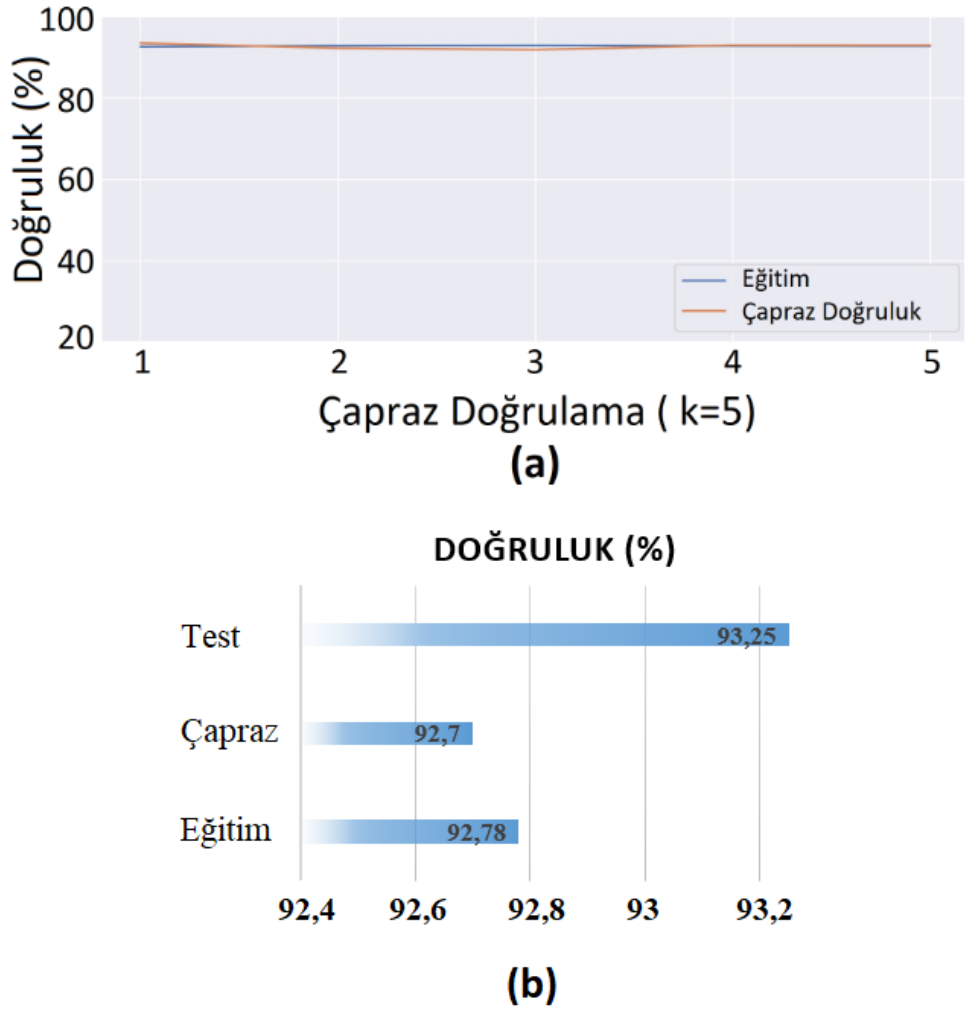
$$\text{Kes} = \frac{\text{DP}}{\text{DP+YP}} \tag{6}$$

$$\text{Geri Çğr} = \frac{DP}{DP+YN} \tag{7}$$

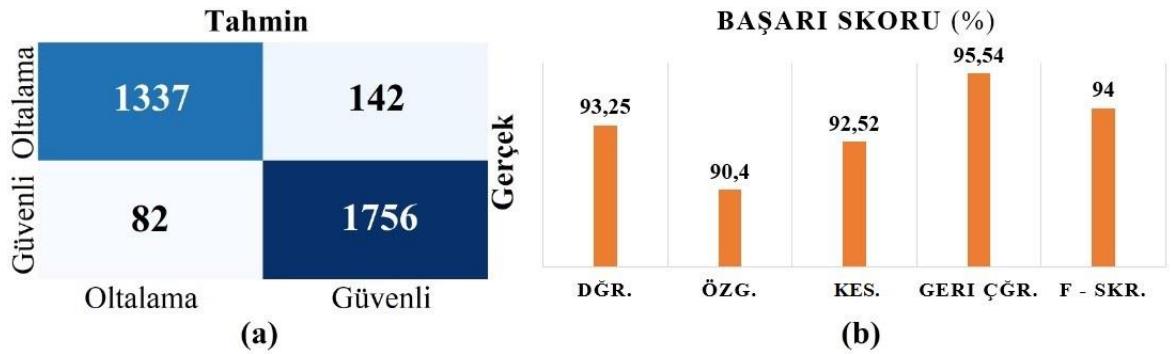
$$\text{F-skr} = \frac{2x\ (\text{Geri Çğr x Kes})}{\text{Geri Çğr+Kes}} \tag{8}$$

$$\text{Dğr} = \frac{DP+DN}{DP+DN+YP+YN} \tag{9}$$

Çalışmanın deneyinde veri seti, eğitim - çapraz doğrulama ve eğitim - test verisi olarak analiz edildi. Dört makine öğrenme yöntemi deney analizi gerçekleştirildi. İlk olarak DVM yöntemi ile analizler gerçekleştirildi. DVM yöntemi ile eğitim verisinde elde edilen doğruluk oranı %92,78'di; çapraz doğrulama başarı oranı %92,70'di ve test verilerinden elde edilen doğruluk oranı %93,25'di. Bu çalışmanın DVM yöntemi ile analizinden elde edilmiş, eğitim - çapraz doğrulama grafiği ve eğitim - çapraz doğrulama - test çubuk grafikleri Şekil 3'te gösterildi. Test verilerinin karmaşıklık matrisini gösteren grafik ve diğer metrik başarı sonuçları ise Şekil 4'te gösterildi.

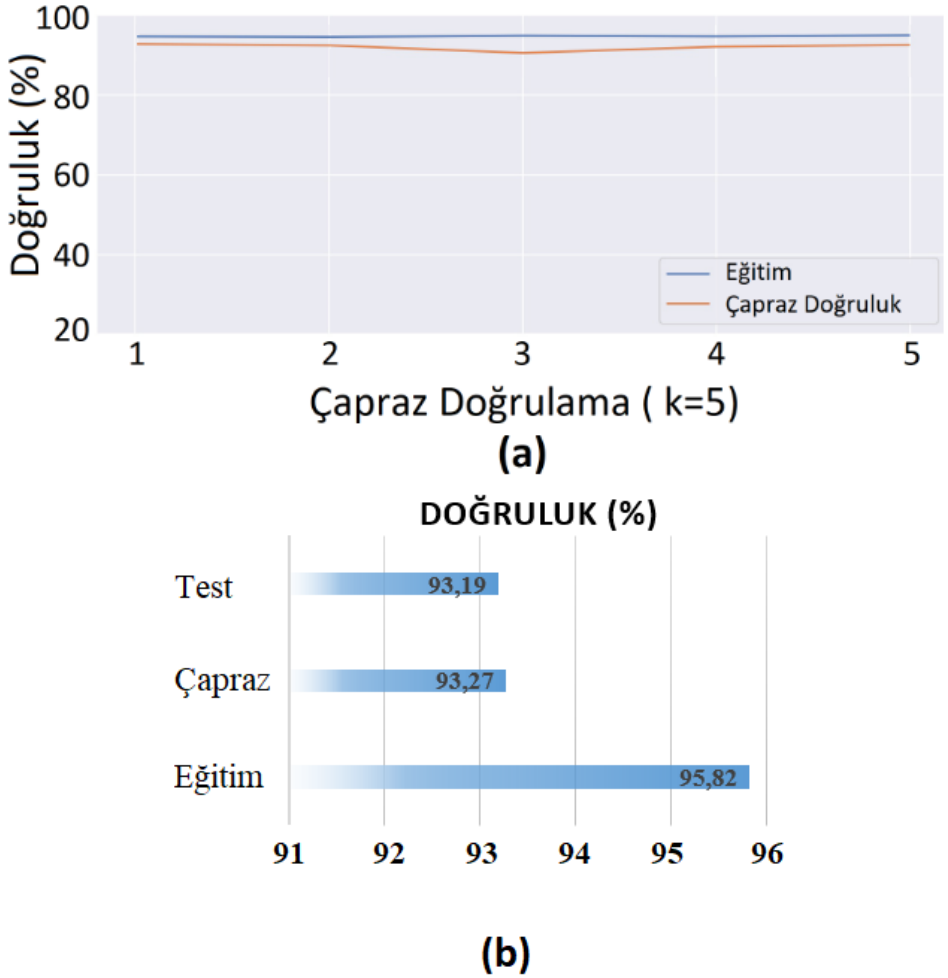


Şekil 3. DVM yöntemi ile elde edilen doğruluk grafikleri;
a) eğitim – çapraz doğrulama, b) eğitim – çapraz doğrulama ve test grafikleri

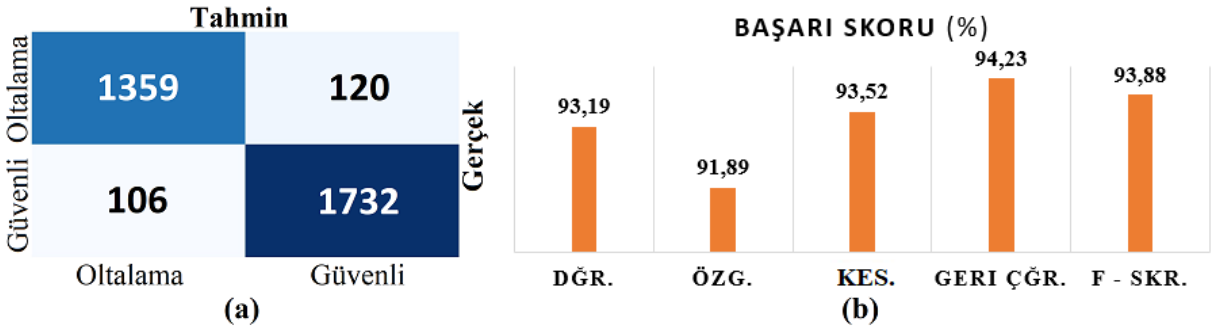


Şekil 4. DVM yöntemi ile test verilerin analiz sonuçları;
a) karmaşıklık matrisi, b) karmaşıklık matrisin metrik sonuçları

İkinci analizde, EYK yöntemi kullanıldı. EYK yöntemi ile eğitim verisinde elde edilen doğruluk oranı %95,82'di; çapraz doğrulama başarı oranı %93,27'di ve test verilerinden elde edilen doğruluk oranı %93,19'du. Bu çalışmanın DVM yöntemi ile analizinden elde edilmiş, eğitim - çapraz doğrulama grafiği ve eğitim - çapraz doğrulama - test çubuk grafikleri Şekil 5'te gösterildi. Test verilerinin karmaşıklık matrisini gösteren grafik ve diğer metrik başarı sonuçları ise Şekil 6'da gösterildi.

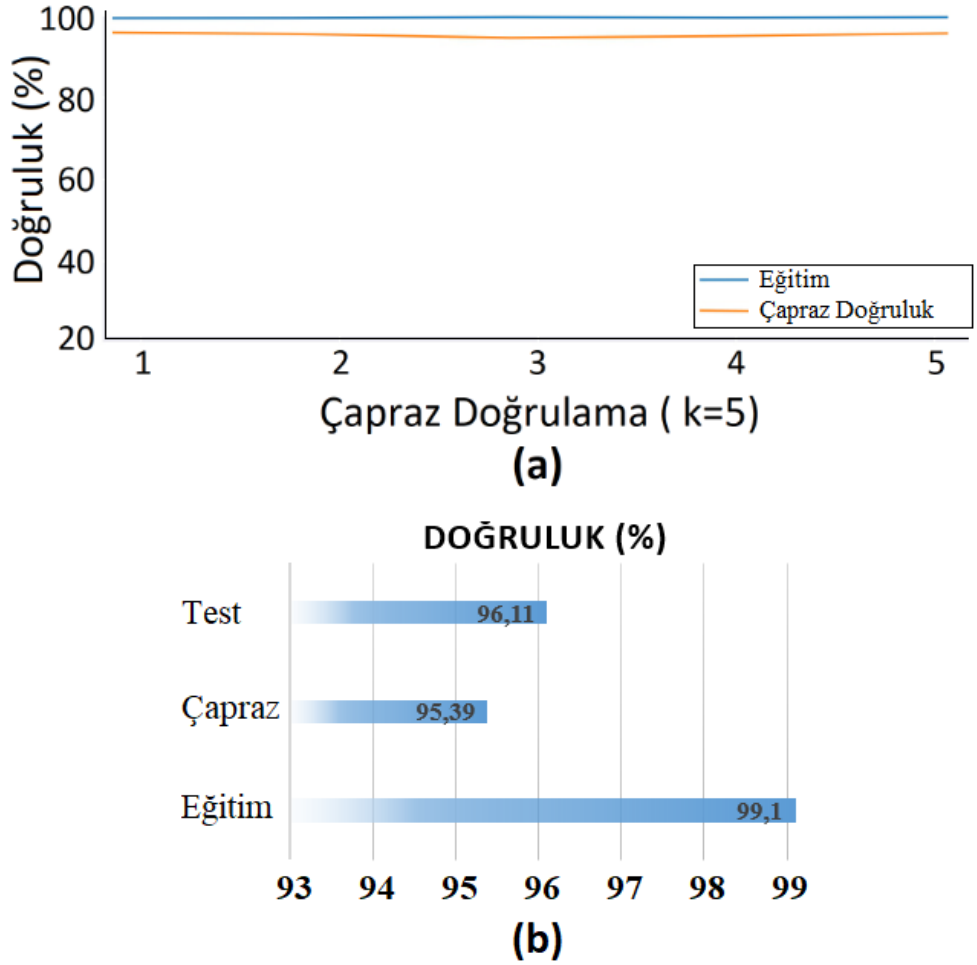


Şekil 5. EYK yöntemi ile elde edilen doğruluk grafikleri;
a) eğitim – çapraz doğrulama, b) eğitim – çapraz doğrulama ve test grafikleri

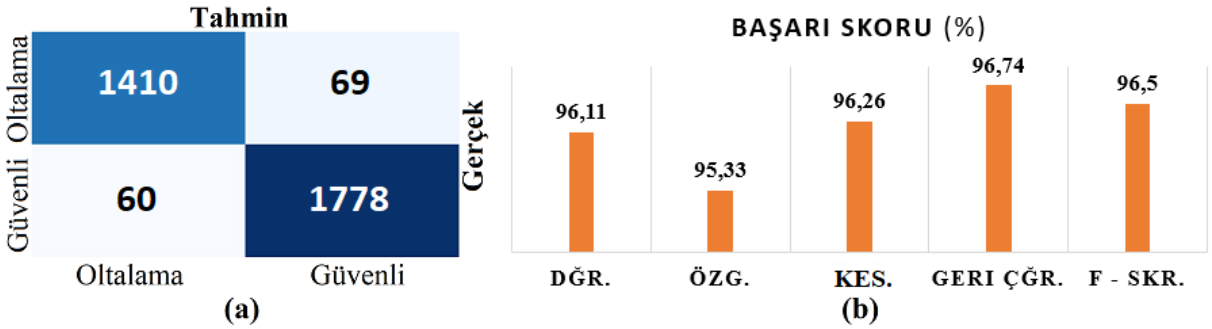


Şekil 6. EYK yöntemi ile test verilerin analiz sonuçları;
a) karmaşıklık matrisi, b) karmaşıklık matrisin metrik sonuçları

Üçüncü analizde, KA yöntemi kullanıldı. KA yöntemi ile eğitim verisinde elde edilen doğruluk oranı %99,1'di; çapraz doğrulama başarı oranı %95,39'dı ve test verilerinden elde edilen doğruluk oranı %96,11'di. Bu çalışmanın DVM yöntemi ile analizinden elde edilmiş, eğitim - çapraz doğrulama grafiği ve eğitim - çapraz doğrulama - test çubuk grafikleri Şekil 7'de gösterildi. Test verilerinin karmaşıklık matrisini gösteren grafik ve diğer metrik başarı sonuçları ise Şekil 8'de gösterildi.

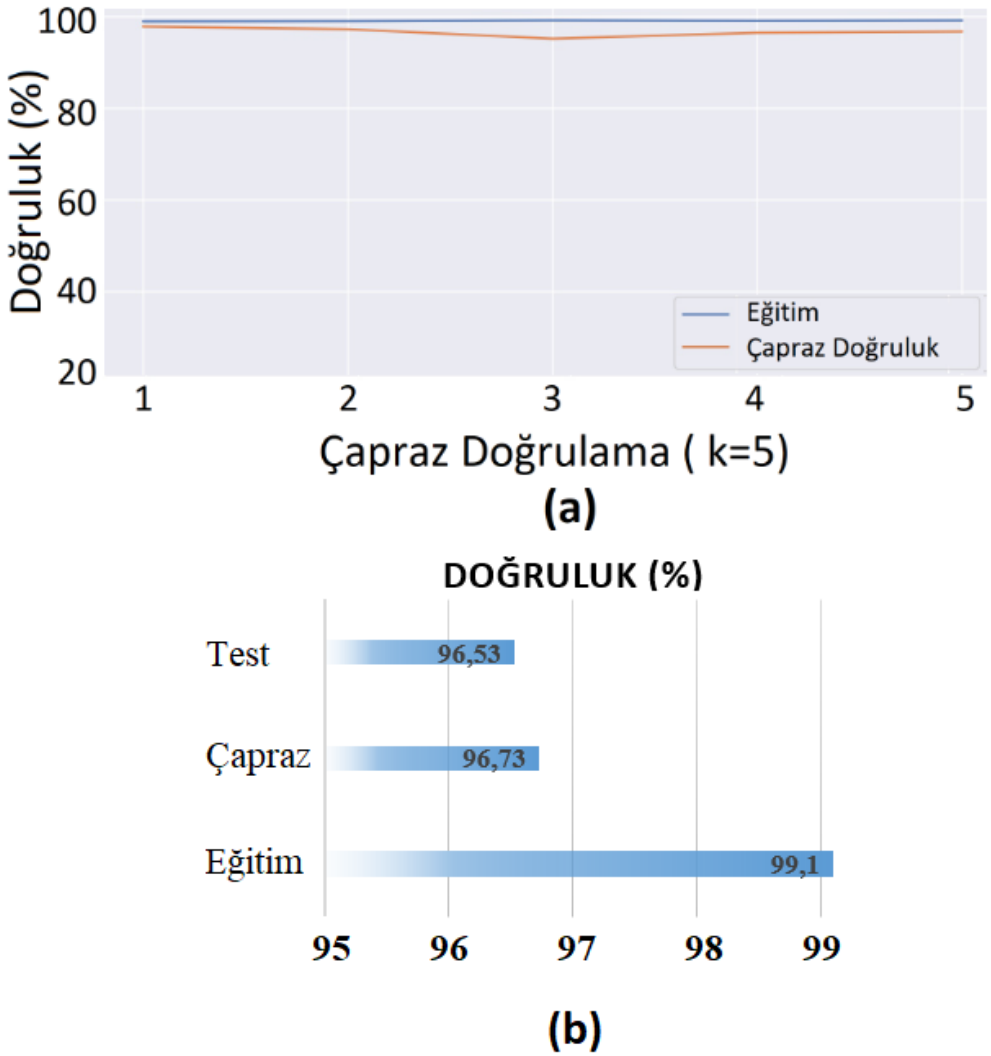


Şekil 7. KA yöntemi ile elde edilen doğruluk grafikleri;
a) eğitim – çapraz doğrulama, b) eğitim – çapraz doğrulama ve test grafikleri

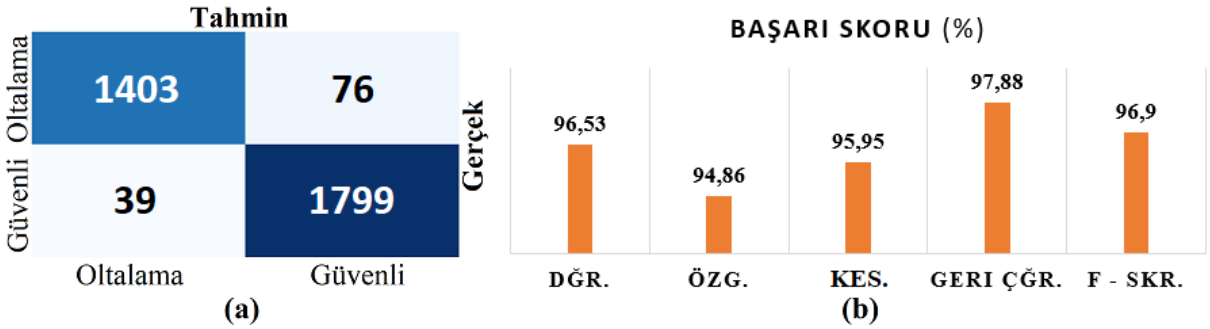


Şekil 8. KA yöntemi ile test verilerin analiz sonuçları;
a) karmaşıklık matrisi, b) karmaşıklık matrisin metrik sonuçları

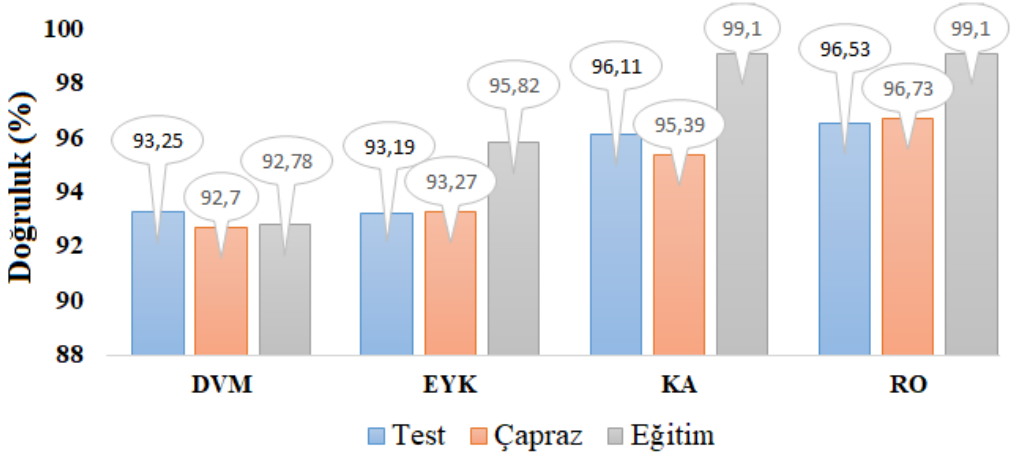
Son analizde, RO yöntemi kullanıldı. RO yöntemi ile eğitim verisinde elde edilen doğruluk oranı %99,10'dı; çapraz doğrulama başarı oranı %96,73'tü ve test verilerinden elde edilen doğruluk oranı %96,53'tü. Bu çalışmanın DVM yöntemi ile analizinden elde edilmiş, eğitim - çapraz doğrulama grafiği ve eğitim - çapraz doğrulama - test çubuk grafikleri Şekil 9'da gösterilmiştir. Test verilerinin karmaşıklık matrisini gösteren grafik ve diğer metrik başarı sonuçları ise Şekil 10'da gösterildi. Ayrıca dört yöntemin doğruluk başarılarını gösteren grafik Şekil 11'de gösterildi. Çalışmanın deneysel analizleri bize RO yönteminin web sitesinde gerçekleştirilen oltalama saldırılarının tespitinde daha etkin olduğunu gösterdi.



Şekil 9. RO yöntemi ile elde edilen doğruluk grafikleri;
a) eğitim – çapraz doğrulama, b) eğitim – çapraz doğrulama ve test grafikleri



Şekil 10. RO yöntemi ile test verilerin analiz sonuçları;
a) karmaşıklık matrisi, b) karmaşıklık matrisin metrik sonuçları



Şekil 11. Deneysel analizlerde kullanılan makine öğrenme yöntemlerinin doğruluk başarı grafikleri

5. Tartışma

Bu makalede, web siteleri üzerinde bilgi güvenliğini tehdit eden oltalama saldırılarının tespitini gerçekleştirildi. Çalışmanın makine öğrenme yöntemleri ile elde ettiği performans sonuçları umut verici oldu. Fakat daha iyi analizler edebilmek için önerdiğimiz yaklaşımı farklı metotlar ile geliştirilmesi gerekir. Önerilen yaklaşımın sınırlı yönleri arasında derin öğrenme modelleri ile makine öğrenme yöntemleri birlikte kullanılması belki de analiz sonuçlarına katkı sunabilirdi. Öte yandan, önerilen yaklaşımın Python kütüphanelerini kullanarak makine öğrenme yöntemleri ile kıyaslatıldı. Burada, veri seti için test-eğitim ve çapraz doğrulama yöntemlerini kullanarak analiz sonuçların güvenirliği sağlamlaştırıldı. Çalışmaya benzer veri setleri kullanarak gerçekleştirilen analizler son zamanlarda yapılmıştır. Bu çalışmalar ile ilgili analiz sonuçları Tablo 2'de verildi.

Tablo 2. Benzer veri seti ile gerçekleştirilmiş çalışmaların karşılaştırılması

Makale	Yıl	Veri seti durumu	Model / Yöntem	Dğr. (%)
Mustafa Kaytan vd. [6]	2017	Çapraz Doğrulama (k=10)	Derin Öğrenme / AÖM	95,93
Ö. Koray Şahingöz vd. [21]	2019	Eğitim ve test verisi	Doğal Dil İşleme / RO	97,98
M. Ali Koşan vd. [22]	2018	Eğitim ve test verisi	RO	97,3
Bu çalışma	2021	Çapraz Doğrulama (k=5)	Makine Öğrenme Yöntemleri	**96,73**
		Test oranı (%30)		**96,53**

Mustafa Kaytan vd. [6] çalışmasında iki sınıflı veri seti kullandılar. Onlar, çalışmasında kullandıkları veri setini yalnızca çapraz doğrulama (k=10) ile analiz ettiler. Kullandıkları veri setindeki her bir web sitesinin 30 özelliği vardı. Bizim çalışmamızdaki veri seti özellik sayısı da 30'du. Burada analiz için tercih ettikleri makine öğrenme yönteminin (AÖM), bizim RO yöntemine göre sınıflandırma performansı düşük olması analiz sonucunu da etkilemiştir. Onlar farklı makine öğrenme yöntemleri ile sınıflandırma yapabilseydi mevcut elde ettikleri başarıyı artırabilirdi. Bu çalışmada çapraz doğrulama yöntemi kullanılarak analizler gerçekleşti. Burada çapraz doğrulama değeri beş seçilmesine rağmen elde edilen sınıflandırma başarısı %96,73'tü. Sonuç olarak doğruluk başarısı çapraz doğrulama yöntemi ile daha da arttırıldığı gözlemlendi. Koray Şahingöz vd. [21] web adreslerinden gerçekleştirilen oltalama saldırılarının tespiti için doğal dil işleme yaklaşımı ile birlikle makine öğrenme yöntemlerini kullandılar. Onlar bu çalışmadan farklı olarak veri setinde kelimelerin birbiriyle ilişkilerini ortaya koyabilen doğal dil işleme yaklaşımını kullandılar. Ardından sınıflandırma işlemini gerçekleştirebilmek için doğal dil işleme yaklaşımı ile analizleri gerçekleştirilen veri setini girdi olarak makine öğrenme yöntemlerine verdiler. En iyi analiz sonucunu RO yöntemi ile elde ettiler. Onların elde ettiği genel doğruluk başarısı %97,98'di. Doğal dil işleme yaklaşımının doğruluk başarısına katkı sağladığı gözlemlenmiştir. Ali Koşan vd. [22] web sitelerinde gerçekleştirilen oltalama saldırılarının tespiti için makine öğrenme yöntemlerini kullandılar. Onlar, weka yazılımını kullanarak sınıflandırma işlemini gerçekleştirmişlerdir. Deneysel analizlerde RO yöntemi diğer yöntemlere göre daha başarılı sonuç üretmiştir. Benzer veri setlerinde klasik makine öğrenme yöntemleri arasında RO yönteminin daha etkili olduğu gözlemlenmiştir.

6. Sonuç ve Öneriler

Bu makalenin deneysel analizinde, web saldırılarının gerçekleştiği oltalama saldırılarının (e-dolandırıcılık) tespitinde yapay zekâ modellerinin ne kadar etkin olduğunu gözlemledik. Günümüzde milyarlarca kullanıcısı olan internet ortamında bu tür saldırılar sıklıkla görülmüştür [23] ve bu saldırıları minimize edebilmek için teknolojik gelişmelerle eş zamanlı olan yazılımları kullanmaktan geçmektedir. Çalışmanın analizinde yapay zekâ tabanlı makine öğrenme yöntemleri sınıflandırma işlemini gerçekleştirmek için kullanıldı. Makine öğrenme yöntemleri arasında en iyi performansı RO yöntemi verdi. RO yöntemi ile elde edilen doğruluk başarısı %96,53'tü. RO yönteminin diğer metrik başarıları ise; özgünlük başarısı %94,86'dı, duyarlılık başarısı %95,95'ti, geri çağırma başarısı %97,88'di ve F1-skor başarısı %96,90'dı.

Gelecek çalışmada, web uygulamalarında gerçekleştirilen oltalama saldırıları için daha geniş özellikli veri setleri araştırılacaktır. Makine öğrenme yöntemlerinin yanında derin öğrenme modelleri, özellik seçme algoritmaları ile birlikte hibrit yaklaşımlar tasarlanarak analizler gerçekleştirilecektir.

Araştırma ve Yayın Etiği Beyanı

Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.

Kaynaklar

[1] Önal H. 2021. Phishing (Oltalama) Saldırısı Nedir? | BGA Security. In: BGA Secur. https://www.bgasecurity.com/2019/09/phishing-oltalama-saldirisi-nedir/. (Erişim: 10 Haziran 2021).

[2] Wei B., Hamad R.A., Yang L., vd. 2019. A Deep-Learning-Driven Light-Weight Phishing Detection Sensor. Sensors (Basel), 19 :4258

[3] Phishing Statistics: The 29 Latest Phishing Stats to Know in 2020 - Hashed Out by The SSL StoreTM. In: Hashedout. https://www.thesslstore.com/blog/phishing-statistics-latest-phishing-stats-to-know/. (Erişim: 19 Haziran 2021).

[4] Abdelhamid M. 2020. The Role of Health Concerns in Phishing Susceptibility: Survey Design Study. J Med Internet Res 22:e18394.

[5] Yi P., Guan Y., Zou F., vd. 2018. Web phishing detection using a deep learning framework. Wirel Commun Mob. Comput., 4678746.

[6] Kaytan M., Hanbay D. 2017. Effective classification of phishing web pages based on new rules by using extreme learning machines. Anatol J Comput Sci, 2:15–36.

[7] Sonowal G. 2020. Phishing email detection based on binary search feature selection. SN Comput Sci, 1:191.

[8] Chand E. 2021. Phishing website Detector. In: Kaggle. https://www.kaggle.com/eswarchandt/phishing-website-detector. (Erişim: 7 Haziran 2021).

[9] Huang S., Cai N., Pacheco P.P., vd. 2017. Applications of support vector machine (SVM) learning in cancer genomics. Cancer Genomics Proteomics, 15: 41–51.

[10] Sertkaya M.E., Ergen B., Togacar M. 2019. Diagnosis of Eye Retinal Diseases Based on Convolutional Neural Networks Using Optical Coherence Images. In: 2019 23rd International Conference Electronics, 1–5.

[11] Erdoğmuş P., Çolak B., Durdağ Z. 2016. K-Means algoritması ile otomatik kümeleme. El-Cezeri J. Sci. Eng. 3:0.

[12] Moghtadaiee V., Dempster A.G. 2015. Determining the best vector distance measure for use in location fingerprinting. Pervasive Mob Comput, 23: 59–79.

[13] Topîrceanu A., Grosseck G. 2017. Decision tree learning used for the classification of student archetypes in online courses. Procedia Comput Sci, 112: 51–60.

[14] Bulut F. 2017. Different mathematical models for entropy in ınformation theory. Bilgi Kuramı ndaki Entropi Kavramıyla İlgili Farklı Matematiksel Modeller, 1: 167–174.

[15] Seifert S. 2020. Application of random forest based approaches to surface-enhanced Raman scattering data. Sci Rep 10:5436.

[16] Aldrich C. 2020. Process variable importance analysis by use of random forests in a shapley regression framework. Minerals, 10: 1–17.

[17] Khan S.A. 2020. Phishing Websites Classification using Deep Learning. In: GitHub. https://github.com/sohailahmedkhan173/Phishing-Websites-Classification-using-Deep-Learning. (Erişim: 9 Haziran 2021).

[18] Google Colab Notebooks- Colaboratory. In: Google. https://colab.research.google.com/notebooks/intro.ipynb. (Erişim: 9 Haziran 2021).

[19] Tumen V., Yildirim O., Ergen B. 2018. Recognition of road type and quality for advanced driver assistance systems with deep learning. Elektron ir Elektrotechnika, 24 :67–74.

[20] Tümen V., Ergen B. 2020. Intersections and crosswalk detection using deep learning and image processing techniques. Physica A: Statistical Mechanics and its Applications, 543: 123510.

[21] Sahingoz Ö.K., Buber E., Demir Ö., Diri B. 2019. Machine learning based phishing detection from URLs. Expert Systems with Applications, 117: 345–357.

[22] Koşan M.A., Yıldız O., Karacan H. 2018. Comparative analysis of machine learning algorithms in detection of phishing websites. Pamukkale University Journal of Engineering Sciences 24 (2): 276–282.

[23] Lin T., Capecci D.E., Ellis D.M., vd. 2019. Susceptibility to spear-phishing emails: effects of internet user demographics and email content. ACM Trans Comput Hum Interact, 26: 32.